MONÉTIQUE

le "tout IP" est sur les rails

Yvon Avenel

Journaliste
Éditeur de
SmartcardTrends

La généralisation de réseaux basés sur IP (Internet Protocol) réduit les coûts mais l'ouverture à un large public crée des problèmes de sécurité et de disponibilité.

Après l'an 2000, l'Euro, CB5.2, EMV, un nouveau chantier ? Oui, et sans doute et pas le moins important. À l'échelle hexagonale bien sûr, et à terme nécessairement, européenne. La généralisation de réseaux ouverts basés sur IP (**Internet Protocol**) pour assurer les échanges et le transport des transactions accepteurs-acquéreurs aura sans doute des conséquences importantes. Cette évolution en effet n'est pas seulement un changement technique de moyens de communications. Il ne s'agit pas de remplacer simplement des liaisons à faibles débits, et coûteuses, utilisant encore le réseau commuté (RTC) et le réseau Transpac, par des liaisons rapides et économiques de type ADSL ou GPRS. C'est un modèle économique nouveau qui se met en place et un paradigme qui peut-être à terme pourrait changer de formule : le on-line va-t-il reprendre une partie des droits que lui avait confisquée par la force des choses depuis vingt ans le modèle très franco-français du off-line ? La monétique intégrée, centralisée via des réseaux locaux IP déjà en place dans les grandes enseignes, ou mise en œuvre en mode hébergée (ASP) via des réseaux distants, encore IP, dans le commerce de détail ou le commerce organisé, a déjà apporté des bribes de réponses. Mais les évolutions des terminaux de paiement – entre PC et PDA, de plus en plus "intelligents" et sécurisés – en apportent d'autres. Pour l'heure, les questions se portent en priorité sur les échéances proches d'un chantier qui concerne bien sûr au premier chef les banques et leurs back-offices, le commerce, mais aussi les opérateurs télécoms et internet, les transporteurs de transactions monétiques (et autres types de transactions d'ailleurs), les processeurs, les fabricants de terminaux de paiement et un certain nombre de prestataires de services. Qui fait quoi ? Surtout comment transformer un système bien connu, éprouvé, qui marche, en un système encore mal connu qui doit marcher sinon mieux, en tout cas, au moins aussi bien que le précédent ? Le système est éminemment complexe. Son évolution ne le sera pas moins.

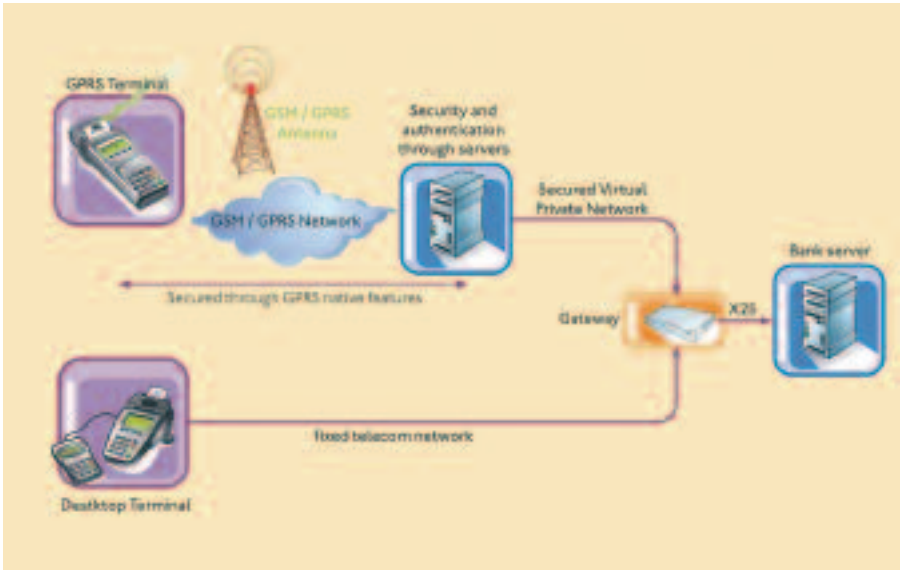
UN SYSTÈME À GÉRER DE BOUT EN BOUT

La généralisation de l'IP dans les réseaux monétiques ne sera pas la mise en œuvre ex-nihilo d'un nouveau système de communication. "*Nous en sommes déjà à notre deuxième génération de terminaux IP, et la demande s'élargit*" souligne Chis Lomax, le responsable du marketing pour l'Europe de VeriFone, "*ce sont les mêmes librairies IP qui sont utilisées pour les liaisons filaires de type Ethernet, ou sans fil en GRPS ou Wi-Fi*". Tous les grands fabricants de terminaux de paiement ont aujourd'hui une offre IP. Celle-ci est d'ailleurs peut-être paradoxalement plus tirée par les applications sans fil (GPRS, Dect, Bluetooth) que filaires (Ethernet). Et même si le parc de ces terminaux n'est pas totalement opérationnel en IP, il l'est potentiellement. Thierry Jasserand, le directeur commercial et marketing de TNS, l'un des plus importants opérateurs mondiaux de transport de transactions monétiques, remarque en effet que le temps moyen de 13 secondes constaté pour une autorisation sur près de 25 % du parc de terminaux français, indique à l'évidence

LES TERMINAUX DE PAIEMENT SONT PRÊTS POUR LA MONÉTIQUE IP

■ **Des expériences pilotes** sont lancées sur la mise en œuvre de terminaux de paiement utilisant des liaisons filaires ou GPRS sans fil.

ARCHITECTURE SIMPLIFIÉE D'UN RÉSEAU FILAIRE ET GPRS



La technologie GPRS semble même gagner les terminaux fixes traditionnellement filaires.

que les modems V.22 et V.32 actifs sont encore légion. Mais à ce niveau, le passage à l'IP pourra se résumer à un simple changement de "prise".

LES LIAISONS IP DÉJÀ ACTIVES DANS LA GRANDE DISTRIBUTION

Actives, les liaisons IP le sont déjà à une autre échelle, dans la grande distribution qui fut l'initiateur en France du mouvement des "pro-IP". "*Auchan qui s'est équipé de notre système de monétique intégrée – des postes clients pour les terminaux de paiement reliés à un réseau local Ethernet à des serveurs de transactions – fait de l'IP de bout-en-bout déjà depuis longtemps*" explique Marc Le Mouel, le directeur général de MoneyLine qui revendique la première place sur le marché de la monétique intégrée pour le commerce organisé en France. Les grandes enseignes ont vite perçu l'intérêt économique et stratégique de l'IP.

UN GAIN EN COÛTS ET EN QUALITÉ DE SERVICE

L'architecture "historique" construite selon le principe des terminaux grappés autour d'un concentrateur et d'un serveur correspondant communiquant via Transpac et (X25 ou Frame Relay) vers les serveurs bancaires d'autorisations, de télécollectes et de paramétrages, n'a plus cours : trop chère [1], pas assez rapide et offrant une visibilité médiocre en matière de gestion. Les flux monétiques sont désormais centralisés vers des serveurs spécialisés communiquant avec les terminaux de paiement IP mis en réseau (Ethernet/IP) grâce à des VPN (Virtual private network). L'une des grandes chaînes françaises de distribution est ainsi en train de s'équiper d'un serveur monétique (le système est redondant) chargé de la télécollecte de ses 70 magasins. Il va remplacer les 140 collectes par jour effectuées jusque-là par chacun des serveurs associés à chacun de ces magasins, par une seule et unique opération de télécollecte. Avec, à la clé, des gains en coûts et des avantages en termes de gestion et de reporting [2], puisque les serveurs chargés d'acheminer les transactions sont généralement associés à des bases de données et des outils de supervision qui rendent accessibles, via un simple navigateur web (un autre avantage de l'IP), des informations qu'il serait plus difficile souvent de retrouver localement. Cela sera encore plus vrai pour les commerces autonomes qui, aujourd'hui, sont loin d'avoir franchi le pas de l'IP, mais qui pourraient en tirer parti pour accéder à des solutions hébergées (ASP) mutualisées sur des serveurs. Finis les travaux manuels de réconciliation et vérification des caisses…

À l'autre bout de la chaîne complète du système de transactions, les serveurs bancaires d'autorisations, de télécollectes ou de paramétrages, qu'ils soient confiés à des tierces parties (les "processeurs") ou gérés en interne, ne sont encore aujourd'hui en majorité accessibles qu'en X25. À quelques exceptions près pourtant, – et elles ne sont pas négligeables lorsque l'on sait le rôle joué par les nouveaux opérateurs de transport monétique –, comme celles des réseaux et les serveurs de TNS qui sont désormais capables d'acheminer de façon transparente les flux monétiques, soit en IP, soit en X25 (XOT). L'opérateur s'est fait une spécialité des conversions de formats et de protocoles. "*Notre rôle est de faciliter ces liaisons à tous les niveaux*" souligne Thierry Jasserand, "*nous sommes à la croisée des chemins entre les banques et le commerce, nous voulons accompagner le développement de l'IP dans la monétique française*".

La situation reste complexe : le déploiement de la monétique IP fait face à de nombreux acteurs dont certains sont de nouveaux entrants, à une situation sur le terrain très contrastée en termes de développements et de moyens de transports IP (VPN, GPRS, Internet, etc.), mais aussi à des problématiques nouvelles en termes de sécurité et disponibilité du réseau. Heureusement, il y a un pilote dans l'"avion".

AVEC LE PILOTAGE GROUPEMENT DES CARTES BANCAIRES "CB"

Pour l'heure en effet, il s'agit en France, de coordonner le mouvement et de tirer les premières leçons des pilotes IP lancés sur le terrain depuis quelques mois. Ces pilotes portent sur la mise en œuvre de plusieurs milliers de terminaux de paiement IP utilisant des liaisons IP/ADSL filaires, et d'un nombre un peu plus important de terminaux utilisant des liaisons GPRS sans fil. La technologie GPRS semble même gagner les terminaux fixes traditionnellement filaires. Les résultats devraient être connus à la fin du premier semestre, indique-t-on au Groupement des Cartes Bancaires "CB", qui assure depuis le début le pilotage de l'opération en coordination avec les représentants de banques, du commerce et les industriels concernés (les fabricants de terminaux, et les opérateurs télécoms notamment). Lancée il y a environ un an cette initiative a été marquée par une étape importante en juin dernier : la publication, par le Groupement des Cartes

Bancaires "CB" de deux documents. Le premier décrit la mise en œuvre protocolaire de CB2A/CB Com sur TCP/IP. Le second énonce un certain nombre d'exigences (encadré) en matière de sécurité. "*Le premier document est le fruit d'un travail mené en étroite concertation avec les représentants des banques et du commerce et les industriels, pour assurer, a minima, en restant très près de l'ISO8583, l'adaptation des protocoles CB sur une pile IP; le second est beaucoup plus un travail qui entre naturellement dans le cadre des missions régaliennes du Groupement, puisqu'il touche à la sécurité*" explique un responsable Groupement des Cartes Bancaires "CB".

LA SÉCURITÉ : LE PREMIER CHALLENGE

La sécurité est en effet l'un des problèmes les plus cruciaux à résoudre. "*Comment sécuriser un réseau ouvert ? Le voilà le vrai défi*" souligne Michel Léger, le responsable de l'activité terminaux de paiements chez Axalto, qui voit dans l'évolution vers le tout IP des opportunités pour mettre en œuvre des solutions basée sur des cartes à puce, et ne craint pas d'imaginer des terminaux de paiements IP "légers" (autour d'un simple navigateur) sur le modèle des clients légers (*thin client*) du monde de la bureautique. "*Où met-on l'intelligence et les services à valeur ajoutée ? Les serveurs d'applications existent déjà. Il faut savoir se réinventer. Nous avons toutes les briques pour construire la bonne solution autour d'un cœur sécurisé. C'est là où se trouve notre métier*". "*La sécurité sur les systèmes ouverts pose en effet des problèmes différents de ceux qui se posaient en X25*" rappelle de son côté Vincent Rolland, le vice-président de Banksys, la société belge qui a conduit en Belgique en 2001 la migration vers le tout-IP, aujourd'hui déployée avec succès, "*Avec IP, nous avons moins de problèmes d'engineering qu'avec X25, mais devons être plus pro-actifs en matière de sécurité. La gestion de cette dernière occupe 30 à 40% de nos ressources. Avec X25, nous étions autour de 10%. Il faut faire plus d'audits, être plus vigilants. Mais nous ne sommes pas dans le monde du PC, même si les terminaux de paiements y ressemblent de plus en plus, les données de transactions ne sont pas des fichiers multimédias, et nous savons parfaitement les identifier, ce qui facilite grandement la surveillance et la sécurité*". Banksys a également profité de sa forte intégration verticale, puisque l'opérateur, également transporteur et "processeur" des transactions pour l'ensemble des banques belges, a conçu et développé lui-même ses propres terminaux de paiement. Cette position qui accroît de facto le contrôle sur l'ensemble du système, qui est par ailleurs pourtant ouvert à d'autres serveurs que ceux de Banksys (les cartes et les terminaux sont multi-applications), favorise bien évidemment la gestion de la sécurité sur l'ensemble de la chaîne de paiement.

CHIFFREMENT PAR LE TERMINAL OU LA CARTE À PUCE ?

Le Groupement des Cartes Bancaires "CB" est dans une position un peu différente. Les exigences en matière de sécurité qu'il a établies et publiées mettent également l'accent sur les règles de maintenance et de contrôle des systèmes et équipements, mais elles ne sont pas des spécifications d'implémentations. Elles laissent donc toute latitude aux industriels et aux opérateurs pour concevoir des solutions matérielles et logicielles aptes à sécuriser les réseaux monétiques IP – évidemment conformes aux recommandations –, et plus précisément chaque moyen de transport IP (réseaux privés, réseaux sans fil, Internet, etc.). Du terminal de paiement, voire de sa base sans fil, voire de la carte à puce, au serveur d'autorisation et de télécollecte. VPN ou SSL ? Chiffrement assuré par le terminal ou par la carte à puce? Telle ou telle solution peut en outre plus ou moins bien convenir : les solutions VPN, par exemple, sont bien adaptées aux grandes enseignes et au commerce organisé, mais paraissent assez difficiles à implémenter chez des commerçants autonomes, et à plus forte raison chez des petits commerçants dont le nombre de transactions par jour est peu élevé. Pour des raisons de coûts d'abord [3], mais aussi pour des questions de gestion de clés. Il faut en effet distribuer, dans tous les routeurs du réseau monétique, une clé par commerçant (comme il faut des clés pour chacun des acquéreurs). Ce qui se conçoit pour des milliers de comptes, n'est plus gérable, avec la sécurité souhaitable, s'il s'agit de centaines de milliers de clés. Banksys confronté à cette difficulté a donc choisi, par exemple, de

LES TRAVAUX DU GROUPEMENT CARTES BANCAIRES "CB"

Sécurité sur IP: huit exigences

■ Le document consacré aux "Exigences sécuritaires liées aux évolutions technologiques sur les systèmes d'acceptation" que le Groupement des Cartes Bancaires "CB" a publié en juin 2004, présente huit exigences qui visent à créer un "espace de confiance monétique à l'intérieur duquel les données sont considérées en sécurité". Ces exigences s'appliquent dans la très grande majorité des cas, à toutes les étapes de la chaîne de la transaction : du terminal de paiement au serveur acquéreur en passant par les équipements des opérateurs télécoms ou de services.

■ La première exigence touche à la confidentialité des données, et suppose le recours à des techniques de chiffrement dont la force peut varier selon les types de réseaux IP utilisés. Un VPN (Réseau Privé virtuel) filaire ou sans fil peut être suffisant, tandis qu'un réseau Bluetooth ou Wi-Fi devra réclamer des mécanismes de cryptographie pour renforcer les systèmes natifs de protection.

■ La seconde exigence est la traçabilité de la maintenance monétique. Cela suppose des procédures pour assurer à chaque intervention sur l'une des parties de la chaîne de la transaction, une identification du mainteneur, de l'heure de son intervention et de la nature de son intervention.

■ La troisième exigence est l'intégrité des systèmes monétiques. Pour l'accepteur en particulier, cette exigence implique qu'un contrôle visuel du système de monétique intégrée fasse partie des procédures de surveillance et d'entretien, et que le commerçant ait été sensibilisé aux risques de fraude encourus et aux besoins de vérification de son ou ses terminaux de paiement.

■ Les autres exigences portent sur la protection nécessaire (intégrité, confidentialité, accès) du lien qui est établi de bout en bout entre l'accepteur et l'acquéreur, sur la protection des liens internes à l'acquéreur, sur la restriction des communications, grâce à des mécanismes de filtrage, aux seuls besoins des applications "métiers", sur le durcissement nécessaire des systèmes d'exploitation utilisés. Et elles portent enfin sur l'intégrité et l'authenticité des données téléchargées.

GLOSSAIRE

CBcom
■ Protocole de communication (couche applicative) établi par le Groupement des Cartes Bancaires "CB" qui fait partie, avec CB 2A, des documents établis par Groupement des Cartes Bancaires "CB" et qui précisent comment les systèmes d'acceptation se raccordent et dialoguent avec les systèmes d'autorisations, de téléparamétrages et de télécollectes.

ISO8583
■ Standard de référence pour les transactions bancaires qui définit les champs et les valeurs correspondantes des trames de données échangées. Mais il est rarement utilisé tel quel. Il sert surtout de base à de nombreux autres protocoles propriétaires.

Pile IP
■ Implémentation d'une suite protocolaire IP (Internet Protocol) organisée en couches selon le modèle ISO. Le niveau IP proprement dit correspond à la couche réseau (IPv4 ou IPv6). Ethernet, par exemple (ou Wi-Fi) se trouve ainsi en dessous et correspond à la couche donnée, tandis que TCP (ou UDP) est au-dessus et correspond à la couche transport. Des protocoles comme CBcom (couche applicative) sont placés encore au-dessus de TCP.

X25
■ Protocole de communication intégrant de puissants mécanismes de correction d'erreurs conçu à l'origine pour faire communiquer des terminaux peu "intelligents" avec des grands serveurs via des PAD (*Packet Assembly/Disassembly*).

XOT
■ Protocole permettant d'encapsuler du X25 dans des trames IP.

VPN (*Virtual Private Network*)
■ Réseau privé utilisé par deux ou plusieurs correspondants pour protéger leurs échanges. Ce réseau est basé sur la technique du "tunnel chiffrant" qui est établi après l'authentification mutuelle des correspondants puis échange de clés, et assure la confidentialité et l'intégrité des données échangées.

SSL (*Secure Socket Layer*) ou TLS (*Transport Security Layer*)
■ Suite de protocoles cryptographiques (couche réseau) qui permet de sécuriser les échanges entre deux parties en faisant appel à des mécanismes à clés publiques (avec usage de certificats) et secrètes.
La version 3 permet l'authentification mutuelle de ces deux parties.

télécharger dans les terminaux des commerçants une couche SSL, et imaginé deux scénarios d'ouverture de session sécurisée, selon la puissance de calcul du terminal utilisé.

LA QUALITÉ DE SERVICE DU RÉSEAU : LE DEUXIÈME CHALLENGE

La disponibilité du réseau est également l'un des grands challenges du passage à IP. Là aussi, les différentes options susceptibles d'être retenues ne s'appliquent qu'à des cas de figure bien identifiés. "*Il ne faut pas perdre de vue que la disponibilité d'un réseau monétique n'est pas comparable à celle du réseau internet. C'est de l'ordre de H+4, par J+1*" souligne Thierry Jasserand qui stigmatise à l'avance les offres ADSL de type "Life-Box" – une machine à tout faire – qui risquent de fleurir chez les opérateurs internet généralistes à l'attention du petit commerce. Pour Vincent Rolland, tout est une question de bon compromis entre le prix d'accès au réseau et la qualité du service. Banksys a néanmoins développé pour ses terminaux de paiement une solution pour s'affranchir de ce dilemme. Elle permet de passer sur le réseau commuté si parfois l'internet, via l'adaptateur ADSL, n'était plus tout à coup accessible. L'opération est transparente pour le commerçant et son client. On pourrait imaginer une solution similaire qui utiliserait le réseau GPRS (qui offre quand même par rapport au RTC un débit plus proche de celui de l'ADSL) pour basculer une transaction en cas de défaillance du réseau. Globalement, Vincent Rolland observe que le taux de disponibilité du réseau IP mis en place en Belgique depuis quatre ans est supérieur à celui de l'ancien réseau X25 : "*Nous avons enregistré l'an dernier un taux de 99,98%, contre un taux de 99,95% que nous constatons couramment avec le réseau X25. Et nous parvenons à des temps de transactions, après frappe du PIN, qui sont inférieurs à la seconde*" précise-t-il.

TERMINAUX "DINOSAURES" OU CLIENTS LÉGERS ?

L'exemple de la Belgique est intéressant à plusieurs titres. Au-delà des spécificités du modèle de la mise en œuvre de son réseau de monétique IP, il montre que la généralisation du "tout-IP" n'a pas consommé le divorce du on-line et du off-line, mais au contraire contribué à assurer un mariage plus étroit des deux "philosophies" ou modèles. Par la réduction des coûts du on-line et l'enrichissement fonctionnel des services liés au paiement ou associés à ce dernier, qui supposent une sécurité forte qu'il n'est pas possible d'implémenter seulement dans le réseau. Elle est aussi impérativement réclamée au point d'acceptation.

La monétique intégrée, centralisée, hébergée on-line a de beaux jours devant elle, grâce à l'IP, mais le "réseau n'est pas le terminal". Les terminaux de paiement depuis quelques années connaissent une explosion de leurs capacités mémoires (jusqu'à 20 Mo là où l'on ne comptait il y a une dizaine d'années que 256 ou 512 Ko), de leur puissance de calcul, et de la force des mécanismes de sécurité qu'ils embarquent désormais. Sont-ils devenus des "dinosaures" comme le remarque Georges Lieberman, le président de Xiring ? Cette société, spécialisée dans les lecteurs "légers" de cartes à puce, vient de développer pour les transactions du réseau Sesam Vitale, un lecteur pour les pharmaciens qui se connecte directement de façon autonome et sécurisée sur les serveurs de transactions et d'applications (mode hébergé) de la CNAM et de Xiring en IP/ADSL. "*Il est vrai que la montée en puissance des terminaux est impressionnante, notre dernier modèle embarque 200 MIPS pour le microprocesseur principal, et 50 MIPS pour le cryptoprocesseur chargé de la sécurité*" reconnaît Didier de Lacretelle, le directeur de la stratégie monétique chez Sagem-Monetel, "*mais ces équipements répondent aussi à une forte évolution vers la multiplication des applications à traiter localement, qu'elles soient liées au paiement ou complètement indépendantes. On parle de plus en plus de la matérialisation du ticket commerçant, par exemple*". ■

NOTES

[1] Si on compare en effet les ratios entre les débits d'alors et les tarifications à la distance (lignes spécialisées) ou au volume (Numeris) aux tarifs appliqués aujourd'hui aux forfaits Internet ADSL.
[2] Cette centralisation pourrait même permettre de mettre en place des systèmes d'alerte sur la fraude de cartes et les chèques volés par simple rapprochement des transactions.
[3] Des opérateurs néerlandais proposeraient d'ores et déjà sur leur marché des VPN aux particuliers et petits commerçants pour 15-20 euros/mois.